

# On congruences involving product of variables from short intervals

M. Z. GARAEV

## Abstract

We prove several results which imply the following consequences.

For any  $\varepsilon > 0$  and any sufficiently large prime  $p$ , if  $\mathcal{I}_1, \dots, \mathcal{I}_{13}$  are intervals of cardinalities  $|\mathcal{I}_j| > p^{1/4+\varepsilon}$  and  $abc \not\equiv 0 \pmod{p}$ , then the congruence

$$ax_1 \cdots x_6 + bx_7 \cdots x_{13} \equiv c \pmod{p}$$

has a solution with  $x_j \in \mathcal{I}_j$ .

There exists an absolute constant  $n_0 \in \mathbb{N}$  such that for any  $0 < \varepsilon < 1$  and any sufficiently large prime  $p$ , any quadratic residue  $\lambda$  modulo  $p$  can be represented in the form

$$x_1 \cdots x_{n_0} \equiv \lambda \pmod{p}, \quad x_i \in \mathbb{N}, \quad x_i \leq p^{1/(4\varepsilon^{2/3})+\varepsilon}.$$

For any  $\varepsilon > 0$  there exists  $n = n(\varepsilon) \in \mathbb{N}$  such that for any sufficiently large  $m \in \mathbb{N}$  the congruence

$$x_1 \cdots x_n \equiv 1 \pmod{m}, \quad x_i \in \mathbb{N}, \quad x_i \leq m^\varepsilon$$

has a solution with  $x_1 \neq 1$ .

**2000 Mathematics Subject Classification:** 11A07, 11B50

**Key words:** congruences, small intervals, product of integers.

# 1 Introduction

For a prime  $p$ , let  $\mathbb{F}_p$  denote the field of residue classes modulo  $p$  and  $\mathbb{F}_p^*$  be the set of nonzero elements of  $\mathbb{F}_p$ .

Let  $\mathcal{I}_1, \dots, \mathcal{I}_{2k}$  be nonzero intervals in  $\mathbb{F}_p$  and let  $\mathcal{B}$  be the box

$$\mathcal{B} = \mathcal{I}_1 \times \mathcal{I}_2 \times \dots \times \mathcal{I}_{2k}.$$

We recall that a set  $\mathcal{I} \subset \mathbb{F}_p$  is called an interval if

$$\mathcal{I} = \{L + 1, \dots, L + N\} \pmod{p}$$

for some integers  $L$  and  $N \geq 1$ .

Given elements  $a, b \in \mathbb{F}_p^*$  and  $c \in \mathbb{F}_p$ , we consider the equation

$$ax_1 \cdots x_k + bx_{k+1} \cdots x_{2k} = c; \quad (x_1, \dots, x_{2k}) \in \mathcal{B}. \quad (1)$$

The problem is to determine how large the size of the box  $\mathcal{B}$  should be in order to guarantee the solvability of (1).

The case  $k = 2$  was initiated in the work of Ayyad, Cochrane and Zhang [3], and then continued in [9] and [2]. It was proved in [3] that there is a constant  $C$  such that if  $|\mathcal{B}| > Cp^2 \log^4 p$ , then the equation

$$ax_1x_2 + bx_3x_4 = c; \quad (x_1, x_2, x_3, x_4) \in \mathcal{B}. \quad (2)$$

has a solution, and they asked whether the factor  $\log^4 p$  can be removed. The authors of [9] relaxed the condition to  $|\mathcal{B}| > Cp^2 \log p$  and also proved that (2) has a solution in any box  $\mathcal{B}$  with  $|\mathcal{I}_1||\mathcal{I}_3| > 15p$  and  $|\mathcal{I}_2||\mathcal{I}_4| > 15p$ . The main question for  $k = 2$  was solved by Bourgain (unpublished); he proved that (2) has a solution in any box  $\mathcal{B}$  with  $|\mathcal{B}| \geq Cp^2$ , for some constant  $C$ .

The case  $k \geq 3$  was a subject of investigation of a recent work of Ayyad and Cochrane [1]. They proved a number of results and conjectured that for fixed  $k \geq 3$  and  $\varepsilon > 0$ , if  $a, b, c \in \mathbb{F}_p^*$ , then there exists a solution of (1) in any box  $\mathcal{B}$  with  $|\mathcal{B}| > Cp^{2+\varepsilon}$ , for some  $C = C(\varepsilon, k)$ .

Given two sets  $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ , the sum set  $\mathcal{A} + \mathcal{B}$  and the product set  $\mathcal{AB}$  are defined as

$$\mathcal{A} + \mathcal{B} = \{a + b; a \in \mathcal{A}, b \in \mathcal{B}\}, \quad \mathcal{AB} = \{ab; a \in \mathcal{A}, b \in \mathcal{B}\}.$$

For a given  $\xi \in \mathbb{F}_p$  we also use the notation

$$\xi\mathcal{A} = \{\xi a; a \in \mathcal{A}\},$$

so that the solvability of (1) can be restated in the form

$$c \in a \prod_{i=1}^k \mathcal{I}_i + b \prod_{i=k+1}^{2k} \mathcal{I}_i.$$

In the present paper we prove the following theorems which improve some results of Ayyad and Cochrane for  $k \geq 7$  (see, Table 1 of [1]).

**Theorem 1.** *For any  $\varepsilon > 0$  there exists  $\delta = \delta(\varepsilon) > 0$  such that the following holds for any sufficiently large prime  $p$ : let  $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_{13} \subset \mathbb{F}_p^*$  be intervals with*

$$|\mathcal{I}_i| > p^{1/4-\delta}, \quad i = 1, 2, \dots, 12; \quad |\mathcal{I}_{13}| > p^{1/4+\varepsilon}.$$

*Then for any  $a, b, c \in \mathbb{F}_p^*$  we have*

$$c \in a \prod_{i=1}^6 \mathcal{I}_i + b \prod_{i=7}^{13} \mathcal{I}_i.$$

If we allow  $1 \in \mathcal{I}_{13}$ , then the condition on the size of  $\mathcal{I}_{13}$  can be relaxed to  $|\mathcal{I}_{13}| > p^\varepsilon$ .

**Theorem 2.** *For any  $\varepsilon > 0$  there exists  $\delta = \delta(\varepsilon) > 0$  such that the following holds for any sufficiently large prime  $p$ : let  $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_{13} \subset \mathbb{F}_p^*$  be intervals with  $1 \pmod{p} \in \mathcal{I}_{13}$  and*

$$|\mathcal{I}_i| > p^{1/4-\delta}, \quad i = 1, 2, \dots, 12; \quad |\mathcal{I}_{13}| > p^\varepsilon.$$

*Then for any  $a, b, c \in \mathbb{F}_p^*$  we have*

$$c \in a \prod_{i=1}^6 \mathcal{I}_i + b \prod_{i=7}^{13} \mathcal{I}_i.$$

From Theorem 2 we have the following consequence.

**Corollary 1.** *For any  $\varepsilon > 0$  there exists  $\delta = \delta(\varepsilon) > 0$  such that the following holds for any sufficiently large prime  $p$ : let  $\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_{12} \subset \mathbb{F}_p^*$  be intervals satisfying  $1 \pmod{p} \in \mathcal{I}_{12}$  and*

$$|\mathcal{I}_i| > p^{1/4-\delta}, \quad i = 1, 2, \dots, 11; \quad |\mathcal{I}_{12}| > p^{1/4+\varepsilon}.$$

*Then for any  $a, b, c \in \mathbb{F}_p^*$  we have*

$$c \in a \prod_{i=1}^6 \mathcal{I}_i + b \prod_{i=7}^{12} \mathcal{I}_i.$$

Indeed, if we set

$$\mathcal{I}'_{12} = \{1, 2, \dots, \lfloor p^{1/4+\varepsilon/2} \rfloor\} \pmod{p}, \quad \mathcal{I}_{13} = \{1, 2, \dots, \lfloor p^{\varepsilon/2} \rfloor\} \pmod{p},$$

then under the condition of Corollary 1 we have  $\mathcal{I}_{12} \supset \mathcal{I}'_{12} \mathcal{I}_{13}$ , and the claim follows from the application of Theorem 2.

We remark that we state and prove our results for intervals of  $\mathbb{F}_p^*$  rather than of  $\mathbb{F}_p$  just for the sake of simplicity. Indeed, this restriction is not essential, as any nonzero interval  $\mathcal{I} \subset \mathbb{F}_p$  contains an interval  $\mathcal{I}' \subset \mathcal{I}$  such that  $0 \notin \mathcal{I}'$  and  $|\mathcal{I}'| \geq |\mathcal{I}|/3$ .

In the case  $b = 0$ , the equation (1) describes the problem of representability of residue classes by product of variables from corresponding intervals. We shall consider the case when the variables are small positive integers. It is known from [8] that for any  $\varepsilon > 0$  and a sufficiently large cube-free  $m \in \mathbb{N}$ , every  $\lambda$  with  $\gcd(\lambda, m) = 1$  can be represented in the form

$$x_1 \cdots x_8 \equiv \lambda \pmod{m}, \quad x_i \in \mathbb{N}, \quad x_i \leq m^{1/4+\varepsilon}.$$

Under the same condition, Harman and Shparlinski [11] proved that  $\lambda$  can be represented in the form

$$x_1 \cdots x_{14} \equiv \lambda \pmod{m}, \quad x_i \in \mathbb{N}, \quad x_i \leq m^{1/(4e^{1/2})+\varepsilon}.$$

We shall prove the following result.

**Theorem 3.** *For any  $0 < c_0 < 1$  there exists a positive integer  $n = n(c_0)$  and a number  $\delta = \delta(c_0) > 0$  such that the following holds: let  $c_0 \leq c < 1$  and*

$$\mathcal{A} = \{x \pmod{m}; 1 \leq x \leq m^c, \gcd(x, m) = 1\}.$$

Then the set  $\mathcal{A}^n$  is a subgroup of the multiplicative group  $\mathbb{Z}_m^*$  and

$$|\mathcal{A}^n| > \delta\phi(m).$$

Here, as usual,  $\phi(\cdot)$  is the Euler's totient function,  $\mathbb{Z}_m^*$  is the multiplicative group of invertible classes modulo  $m$  and  $\mathcal{A}^n$  is the  $n$ -fold product set of  $\mathcal{A}$ , that is,

$$\mathcal{A}^n = \{x_1 \cdots x_n; \quad x_i \in \mathcal{A}\}.$$

Recall that  $|\mathbb{Z}_m^*| = \phi(m)$ .

From Theorem 3 we shall derive the following consequences.

**Corollary 2.** *For any  $\varepsilon > 0$  there exists a positive integer  $k = k(\varepsilon)$  such that for any sufficiently large positive integer  $m$  the congruence*

$$x_1 \cdots x_k \equiv 1 \pmod{m}, \quad x_i \in \mathbb{N}, \quad x_i \leq m^\varepsilon$$

*has a solution with  $x_1 \neq 1$ .*

**Corollary 3.** *There exists an absolute constant  $n_0 \in \mathbb{N}$  such that for any  $0 < \varepsilon < 1$  and any sufficiently large prime  $p > p_0(\varepsilon)$ , every quadratic residue  $\lambda$  modulo  $p$  can be represented in the form*

$$x_1 \cdots x_{n_0} \equiv \lambda \pmod{p}, \quad x_i \in \mathbb{N}, \quad x_i \leq p^{1/(4e^{2/3})+\varepsilon}.$$

## 2 Proof of Theorems 1,2

The proof of Theorems 1,2 is based on the arguments of Ayyad and Cochrane [1] with some modifications.

**Lemma 1.** *Let  $N < p$  be a positive integer,  $\mathcal{X} \subset \{1, 2, \dots, p-1\}$ . Then for any fixed integer constant  $n_0 > 0$  we have*

$$|\{xy \pmod{p}; \quad x \in \mathcal{X}, \quad 1 \leq y \leq N\}| > \Delta|\mathcal{X}|,$$

where

$$\Delta = \min\left\{\left(\frac{p}{|\mathcal{X}|}\right)^{1/n_0}, \frac{N}{|\mathcal{X}|^{1/n_0}}\right\} N^{o(1)}$$

as  $N \rightarrow \infty$ .

*Proof.* Let  $J$  be the number of solutions of the congruence

$$x_1 y_1 \equiv x_2 y_2 \pmod{p}, \quad x_1, x_2 \in \mathcal{X}, \quad 1 \leq y_1, y_2 \leq N.$$

Then

$$J = \frac{1}{p-1} \sum_{\chi} \left| \sum_{x \in \mathcal{X}} \chi(x) \right|^2 \left| \sum_{y=1}^N \chi(y) \right|^2.$$

Therefore, by the Hölder inequality we get

$$J \leq A^{(n_0-1)/n_0} B^{1/n_0}, \quad (3)$$

where

$$A = \frac{1}{p-1} \sum_{\chi} \left| \sum_{x \in \mathcal{X}} \chi(x) \right|^{2n_0/(n_0-1)}, \quad B = \frac{1}{p-1} \sum_{\chi} \left| \sum_{y=1}^N \chi(y) \right|^{2n_0}. \quad (4)$$

Next, we have

$$A \leq |\mathcal{X}|^{2/(n_0-1)} \left( \frac{1}{p-1} \sum_{\chi} \left| \sum_{x \in \mathcal{X}} \chi(x) \right|^2 \right) = |\mathcal{X}|^{(n_0+1)/(n_0-1)}.$$

The quantity  $B$  is equal to the number of solutions of the congruence

$$y_1 \cdots y_{n_0} \equiv y_{n_0+1} \cdots y_{2n_0} \pmod{p}, \quad 1 \leq y_i \leq N.$$

We express the congruence as the equation

$$y_1 \cdots y_{n_0} = y_{n_0+1} \cdots y_{2n_0} + pz, \quad 1 \leq y_i \leq N, \quad z \in \mathbb{Z}.$$

Note than  $|z| \leq N^{n_0}/p$ . Hence, there are at most

$$\left( \frac{2N^{n_0}}{p} + 1 \right) N^{n_0}$$

possibilities for  $(y_{n_0+1}, \dots, y_{2n_0}, z)$ . from the estimate for the divisor function it follows that, for each fixed  $y_{n_0+1}, \dots, y_{2n_0}, z$  there are at most  $N^{o(1)}$  possibilities for  $y_1, \dots, y_{n_0}$ . Therefore,

$$B \leq \left( \frac{N^{n_0}}{p} + 1 \right) N^{n_0+o(1)}.$$

Incorporating this and (4) in (3), we obtain

$$J \leq |\mathcal{X}|^{(n_0+1)/n_0} \left( \frac{N}{p^{1/n_0}} + 1 \right) N^{1+o(1)}.$$

Therefore, from the relationship between the number of solutions of a symmetric congruence and the cardinality of the corresponding set, it follows

$$\begin{aligned} & |\{xy \pmod{p}; x \in \mathcal{X}, 1 \leq y \leq N\}| \\ & \geq \frac{|\mathcal{X}|^2 N^2}{J} \geq \min\{|\mathcal{X}|^{(n_0-1)/n_0} p^{1/n_0}, |\mathcal{X}|^{(n_0-1)/n_0} N\} N^{o(1)}, \end{aligned}$$

which concludes the proof of Lemma 1.  $\square$

**Lemma 2.** *Let  $\mathcal{X} \subset \{1, 2, \dots, p-1\}$  and let  $\mathcal{I} \subset \{1, 2, \dots, p-1\}$  be an interval with  $|\mathcal{I}| > p^{1/4+\varepsilon}$ , where  $\varepsilon > 0$ . Then*

$$|\{xy \pmod{p}; x \in \mathcal{X}, y \in \mathcal{I}\}| > 0.5 \min\{p, |\mathcal{X}|p^c\}$$

for some  $c = c(\varepsilon) > 0$ .

*Proof.* As in the proof of Lemma 1, we let  $J$  be the number of solutions of the congruence

$$x_1 y_1 \equiv x_2 y_2 \pmod{p}, \quad x_1, x_2 \in \mathcal{X}, \quad y_1, y_2 \in \mathcal{I}.$$

Then

$$J = \frac{1}{p-1} \sum_{\chi} \left| \sum_{x \in \mathcal{X}} \chi(x) \right|^2 \left| \sum_{y \in \mathcal{I}} \chi(y) \right|^2.$$

Since  $|\mathcal{I}| > p^{1/4+\varepsilon}$ , from the well-known character sum estimates of Burgess [4, 5], we have

$$\left| \sum_{n \in \mathcal{I}} \chi(n) \right| < |\mathcal{I}| p^{-\delta}, \quad \delta = \delta(\varepsilon) > 0,$$

for any non-principal character  $\chi \pmod{p}$ . Therefore, separating the term that corresponds to the principal character  $\chi = \chi_0$ , we get

$$J \leq \frac{|\mathcal{X}|^2 |\mathcal{I}|^2}{p-1} + |\mathcal{I}|^2 p^{-2\delta} \left( \frac{1}{p-1} \sum_{\chi} \left| \sum_{x \in \mathcal{X}} \chi(x) \right|^2 \right) = \frac{|\mathcal{X}|^2 |\mathcal{I}|^2}{p-1} + |\mathcal{X}| |\mathcal{I}|^2 p^{-2\delta}.$$

Hence,

$$|\{xy \pmod{p}; x \in \mathcal{X}, y \in \mathcal{I}\}| \geq \frac{|\mathcal{X}|^2 |\mathcal{I}|^2}{J} \geq 0.5 \min\{p, |\mathcal{X}|p^\delta\}.$$

$\square$

In what follows, the elements of  $\mathbb{F}_p$  will be represented by their concrete representatives from the set of integers  $\{0, 1, \dots, p-1\}$ .

Following the lines of the work of Ayyad and Cochrane [1], we appeal to the result of Hart and Iosevich [12].

**Lemma 3.** *Let  $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$  be subsets of  $\mathbb{F}_p^*$  satisfying*

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > p^3.$$

*Then*

$$\mathbb{F}_p^* \subset \mathcal{A}\mathcal{B} + \mathcal{C}\mathcal{D}.$$

We also need the following consequence of [6, Corollary 18].

**Lemma 4.** *Let  $h < p^{1/4}$  and let  $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3 \subset \mathbb{F}_p^*$  be intervals of cardinalities  $|\mathcal{A}_i| > h$ ,  $i=1,2,3$ . Then*

$$|\mathcal{A}_1\mathcal{A}_2\mathcal{A}_3| \geq \exp\left(-C \frac{\log h}{\log \log h}\right) h^3.$$

*for some constant  $C$ .*

Now we proceed to derive Theorems 1,2. Let  $p^{0.1} < h < p^{1/4}$  to be defined later and assume that

$$|\mathcal{I}_i| > h, \quad i = 1, 2, \dots, 12.$$

Define

$$\mathcal{X} = \mathcal{I}_7\mathcal{I}_8\mathcal{I}_9, \quad \mathcal{A} = \mathcal{I}_1\mathcal{I}_2\mathcal{I}_3, \quad \mathcal{B} = \mathcal{I}_4\mathcal{I}_5\mathcal{I}_6, \quad \mathcal{C} = \mathcal{I}_7\mathcal{I}_8\mathcal{I}_9, \quad \mathcal{D} = \mathcal{X}\mathcal{I}_{13}.$$

From Lemma 4 we have that  $|\mathcal{X}| > h^{3+o(1)}$  and

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}| > h^{9+o(1)}.$$

Now we observe that Lemmas 1,2 imply that

$$|\mathcal{D}| = |\mathcal{X}\mathcal{I}_{13}| > h^{3+\delta_0} \tag{5}$$

for some  $\delta_0 = \delta_0(\varepsilon) > 0$ . Indeed, this is trivial for  $|\mathcal{X}| > h^{3.1}$ , so let  $|\mathcal{X}| < h^{3.1}$ . Then in the case of Theorem 1 the estimate (5) follows from Lemma 2. In



the case of Theorem 2 we apply Lemma 1 with  $N = \lfloor p^\varepsilon \rfloor$  and  $n_0 = \lceil 1/\varepsilon \rceil$ , and obtain that

$$|\mathcal{D}| > |\mathcal{X}||\mathcal{I}_3|^\delta > h^{3+0.9\delta}$$

for some  $\delta = \delta(\varepsilon) > 0$ .

Thus, we have (5), whence

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > h^{12+0.9\delta_0}.$$

Therefore, there exists  $c = c(\varepsilon) > 0$  such that if  $h = p^{\frac{1}{4}-c}$ , then we get

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > p^3.$$

Theorems 1,2 now follow by appealing to Lemma 3.

### 3 Proof of Theorem 3

Let  $\mathcal{G}$  be an abelian group written multiplicatively and let  $\mathcal{X} \subset G$ . The set  $\mathcal{X}$  is a basis of order  $h$  for  $\mathcal{G}$  if  $\mathcal{X}^h = \mathcal{G}$ . This definition implies that if  $1 \in \mathcal{X}$  and  $\mathcal{X}$  is a basis of order  $h$  for  $\mathcal{G}$ , then  $\mathcal{X}$  is also a basis of order  $h_1$  for  $\mathcal{G}$  for any  $h_1 \geq h$ .

We need the following consequence of a result of Olson [13, Theorem 2.2] given in Hamidoune and Rödseth [10, Lemma 1].

**Lemma 5.** *Let  $\mathcal{X}$  be a subset of  $\mathcal{G}$ . Suppose that  $1 \in \mathcal{X}$  and that  $\mathcal{X}$  generates  $\mathcal{G}$ . Then  $\mathcal{X}$  is a basis for  $\mathcal{G}$  of order at most  $\max \left\{ 2, \frac{2|\mathcal{G}|}{|\mathcal{X}|} - 1 \right\}$ .*

We recall that  $\Psi(x; y)$  denotes the number of  $y$ -smooth positive integers  $n \leq x$  (that is the number of positive integers  $n \leq x$  with no prime divisors greater than  $y$ ), and  $\Psi_q(x; y)$  denotes the number of  $y$ -smooth positive integers  $n \leq x$  with  $\gcd(n, q) = 1$ . It is well known that for any  $\varepsilon > 0$  there exists  $\delta = \delta(\varepsilon) > 0$  such that  $\Psi(m; m^\varepsilon) \geq \delta m$ . We need the following lemma, which follows from [7, Theorem 1].

**Lemma 6.** *For any  $\varepsilon > 0$  there exists  $\delta = \delta(\varepsilon) > 0$  such that*

$$\Psi_m(m; m^\varepsilon) > \delta \phi(m).$$

We proceed to prove Theorem 3. Let  $\mathcal{S} = \mathcal{S}(c_0, m)$  be the set of  $m^{c_0}$ -smooth positive integers  $n \leq m$  with  $\gcd(n, m) = 1$ . As mentioned in [11], if  $x \in \mathcal{S}$ , then we can combine the prime divisors of  $x$  in a greedy way into factors of size at most  $m^c$ . More precisely, we can write  $x = x_1 \cdots x_k$  such that  $x_1 \leq m^c$  and  $m^{c/2} \leq x_j \leq m^c$  for  $j = 2, \dots, k$ . In particular, we have

$$(k-1)c_0/2 \leq (k-1)c/2 \leq 1.$$

Hence,  $k \leq 2/c_0 + 1$ , and since  $1 \pmod{m} \in \mathcal{A}$ , it follows that

$$\mathcal{S} \pmod{m} \subset \mathcal{A}^{n_1}; \quad n_1 = \lceil 2/c_0 \rceil + 1.$$

In particular, by Lemma 6 we have

$$|\mathcal{A}^{n_1}| \geq |\mathcal{S}| = \Psi_m(m; m^\varepsilon) > \delta\phi(m) \tag{6}$$

for some  $\delta = \delta(c_0) > 0$ .

Let  $h$  be the smallest positive integer such that  $\mathcal{A}^{n_1 h}$  is a subgroup of  $\mathbb{Z}_m^*$ . Applying Lemma 5 with  $\mathcal{G} = \mathcal{A}^{n_1 h}$  and  $\mathcal{X} = \mathcal{A}^{n_1}$ , we get that

$$h \leq 1 + \frac{2|\mathcal{A}^{n_1 h}|}{|\mathcal{A}^{n_1}|} \leq 1 + \frac{2|\mathbb{Z}_m^*|}{|\mathcal{A}^{n_1}|} \leq 1 + \frac{2\phi(m)}{\delta\phi(m)} = 1 + 2\delta^{-1}.$$

Therefore, since  $1 \pmod{m} \in \mathcal{A}$ , we get that for  $n = (1 + \lceil 2\delta^{-1} \rceil)n_1$  the set  $\mathcal{A}^n$  is a multiplicative subgroup of  $\mathbb{Z}_m^*$ . Taking into account (6), we conclude the proof of Theorem 3.

Let now  $g$  be any element of the group  $\mathcal{A}^n$  distinct from  $1 \pmod{m}$ . We also have that  $g^{-1} \in \mathcal{A}^n$ . Thus, Corollary 2, with  $k = 2n$ , follows from the representation  $gg^{-1} = 1 \pmod{m}$ .

We shall now prove Corollary 3. Let

$$\mathcal{A} = \{x \pmod{p}; x \in \mathbb{N}, x \leq p^{1/(4e^{2/3})+\varepsilon}\}.$$

In Theorem 3, we take  $m = p$ ,  $c_0 = 1/(4e^{2/3})$  and  $c = 1/(4e^{2/3}) + \varepsilon$ . Thus, there is an absolute constant  $n_0$  such that  $\mathcal{A}^{n_0}$  is a subgroup of  $\mathbb{F}_p^*$  and  $|\mathcal{A}^{n_0}| > \delta_0(p-1)$  for some absolute constant  $\delta_0 > 0$ . In other words, there is an integer  $\ell | p-1$  with  $1 \leq \ell \leq 1/\delta_0$  such that

$$\mathcal{A}^{n_0} = \{x^\ell \pmod{p}; 1 \leq x \leq p-1\}.$$

Let  $t = t(\ell, p)$  be the smallest positive  $\ell$ -th power nonresidue modulo  $p$ . According to the well-known consequence of Vinogradov's work [14] combined with the Burgess character sum estimate [4, 5], we have that

$$t \leq p^{1/(4e^{(\ell-1)/\ell})+\varepsilon/2}.$$

On the other hand, since  $t \notin \mathcal{A}^{n_0}$  we have  $t \geq p^{1/(4e^{2/3})+\varepsilon}$ . Hence,  $\ell \in \{1, 2\}$  and the claim follows.

## References

- [1] A. Ayyad and T. Cochrane, *The congruence  $ax_1 \cdots x_k + bx_{k+1} \cdots x_{2k} \equiv c \pmod{p}$* , Proc. Amer. Math. Soc. **145** (2017), 467–477
- [2] A. Ayyad and T. Cochrane, *Lattices in  $\mathbb{Z}^2$  and the congruence  $xy + uv \equiv c \pmod{m}$* , Acta Arith. **132** (2008), no. 2, 127–133.
- [3] A. Ayyad, T. Cochrane and Zh. Zheng, *The congruence  $x_1x_2 \equiv x_3x_4 \pmod{p}$ , the equation  $x_1x_2 = x_3x_4$ , and mean values of character sums*, J. Number Theory **59** (1996), 398–413.
- [4] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. **12** (1962), 179–192.
- [5] D. A. Burgess, *On character sums and  $L$ -series. II.*, Proc. London Math. Soc. **13** (1963), 524–536.
- [6] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, *On congruences with products of variables from short intervals and applications*, Proc. Steklov Inst. Math. **280** (2013), no. 1, 61–90.
- [7] E. Fouvry and G. Tenenbaum, *Entiers sans grand facteur premier en progressions arithmétiques*, Proc. London Math. Soc. (3) **63** (1991), 449–494.
- [8] M. Z. Garaev, *On multiplicative congruences*, Math. Z. **272** (2012), no. 12, 473–482.
- [9] M. Z. Garaev and V. C. García, *The equation  $x_1x_2 = x_3x_4 + \lambda$  in fields of prime order and applications*, J. Number Theory **128** (2008), 2520–2537.

- [10] Y. O. Hamidoune and Ö. J. Rödl, *On bases for  $s$ -finite groups*, Math. Scand. **78** (1996), no. 2, 246–254.
- [11] G. Harman and I. E. Shparlinski, *Products of small integers in residue classes and additive properties of Fermat quotients*, Int. Math. Res. Not. **5** (2016), 1424–1446.
- [12] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, Radon transforms, geometry, and wavelets, 129–135, Contemp. Math., 464, Amer. Math. Soc., Providence, RI, 2008.
- [13] J. E. Olson, *Sums of sets of group elements*, Acta Arith. **28** (1975/76), no. 2, 147–156.
- [14] I. M. Vinogradov, *On the bound of the least non-residue of  $n$ -th powers*, Trans. Amer. Math. Soc. **29** (1927), 218–226.

M. Z. Garaev, Centro de Ciencias Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México.

Email: `garaev@matmor.unam.mx`